

WHAT IS CLAIMED IS:

1 1. A key delivery apparatus that manages a decryption key
2 for decrypting an encrypted content and a suppliable number
3 showing how many times the decryption key is suppliable, with
4 respect to a terminal apparatus connected to a network,
5 comprising:

6 a receiving unit operable to receive, from the terminal
7 apparatus, a supply request for the decryption key;

8 a supply judging unit operable, if the terminal
9 apparatus is a legitimate supply target, to judge whether
10 the terminal apparatus is one of a first-type terminal
11 apparatus that manages a content-usage period and a
12 second-type terminal apparatus that does not manage the
13 content-usage period; and

14 a key supply unit operable, if the suppliable number
15 has a remaining number, to supply to the terminal apparatus,
16 the decryption key and a key-usage period of the decryption
17 key when judged that the terminal apparatus is the first-type
18 terminal apparatus and the decryption key when judged that
19 the terminal apparatus is the second-type terminal apparatus,
20 wherein

21 the supply judging unit judges the terminal apparatus
22 to be the first-type terminal apparatus if the terminal
23 apparatus records the encrypted content, the decryption key,

24 and the key-usage period onto a portable recording medium.

1 2. The key delivery apparatus of claim 1, wherein

2 the network is a home network connected to an external
3 network, contents are received from outside the home network,
4 and the key delivery apparatus judges terminal apparatuses
5 connected to the home network to be legitimate supply
6 targets.

1 3. The key delivery apparatus of claim 1, further comprising:

2 a key-information storage unit operable to store the
3 key-usage period subsequent to supply of the decryption key
4 and the key-usage period to the first-type terminal
5 apparatus;

6 a period judging unit operable to judge whether the
7 key-usage period has expired; and

8 a time management unit operable to add "1" to the
9 suppliable number when judged that the key-usage period has
10 expired.

1 4. The key delivery apparatus of claim 3, further comprising:

2 a date-time storage unit operable to store at least one
3 of a first grouping and a second grouping, the first grouping
4 formed from date-time information showing the key-usage

5 period and a supply date-time of the decryption key, and
6 identification information showing the supply target to be
7 the first-type terminal apparatus, and the second grouping
8 formed from date-time information showing a supply date-time
9 of the decryption key, and identification information
10 showing the supply target to be the second-type terminal
11 apparatus;

12 a date-time judging unit operable to judge whether a
13 present date-time has reached the supply date-time; and

14 a date-time supply unit operable, when judged that the
15 present date-time has reached the supply date-time, to supply
16 the decryption key and the key-usage period to the first-type
17 terminal apparatus or the decryption key to the second-type
18 terminal apparatus, based on the identification information.

1 5. The key delivery apparatus of claim 4, further comprising:

2 a search requesting unit operable to notify, to the
3 first-type terminal apparatus and the second-type terminal
4 apparatus, search information showing the decryption key;
5 and

6 a proprietary information receiving unit operable to
7 receive information indicating that the decryption key is
8 being held, from whichever of the first-type terminal
9 apparatus and the second-type terminal apparatus holds the

10 decryption key.

1 6. The key delivery apparatus of claim 5, wherein
2 the key delivery apparatus stores secret information
3 used as a reference in judging whether the terminal apparatus
4 is a legitimate supply target,
5 the supply judging unit includes an authentication
6 subunit operable to judge whether the terminal apparatus
7 holds the secret information, and
8 the supply judging unit judges the terminal apparatus
9 to be a legitimate supply target when judged that the terminal
10 apparatus holds the secret information.

1 7. The key delivery apparatus of claim 6, wherein
2 the key supply unit includes a remaining number judging
3 subunit operable to judge whether the suppliable number is
4 greater than a predetermined reference number, and
5 the key supply unit judges the suppliable number to have
6 the remaining number when judged that the suppliable number
7 is greater than the predetermined reference number.

1 8. The key delivery apparatus of claim 7, wherein
2 the key supply unit further includes an encryption
3 subunit operable to encrypt the decryption key and the

4 key-usage period when the decryption key and the key-usage
5 period are to be supplied to the first-type terminal
6 apparatus, and to encrypt the decryption key when the
7 decryption key is to be supplied to the second-type terminal
8 apparatus, and

9 the key supply unit, when judged that the suppliable
10 number has the remaining number, supplies to the terminal
11 apparatus, the encrypted decryption key and the encrypted
12 key-usage period when judged that the terminal apparatus is
13 the first-type terminal apparatus and the encrypted
14 decryption key when judged that the terminal apparatus is
15 the second-type terminal apparatus.

1 9. The key delivery apparatus of claim 8, further comprising:

2 a historical information storage unit operable to store
3 historical information showing a connection date-time of the
4 first-type terminal apparatus;

5 a connection judging unit operable to judge, using the
6 connection date-time, whether the first-type terminal
7 apparatus was connected within a predetermined connection
8 period; and

9 a connection management unit operable to add "1" to the
10 suppliable number when judged that the first-type terminal
11 apparatus was not connected within the connection period.

1 10. The key delivery apparatus of claim 8, further
2 comprising:

3 a frequency storage unit operable to store a usage
4 frequency of the decryption key by the first-type terminal
5 apparatus;

6 a frequency judging unit operable to judge whether the
7 usage frequency has reached a predetermined reference
8 frequency; and

9 a connection management unit operable to add "1" to the
10 suppliable number when judged that the usage frequency has
11 reached the reference frequency.

1 11. A terminal apparatus that receives, via a network, supply
2 of a decryption key for decrypting an encrypted content from
3 a key delivery apparatus that manages the decryption key,
4 comprising:

5 a requesting unit operable to request the key delivery
6 apparatus for the decryption key;

7 a key reception unit operable to receive the decryption
8 key from the key delivery apparatus, when judged in the key
9 delivery apparatus that supply of the decryption key is
10 possible;

11 a detecting unit operable to detect an end of content
12 usage conducted using the decryption key; and

13 an end notifying unit operable, when detected that
14 content usage has ended, to delete the decryption key, and
15 notify to the key delivery apparatus, usage-ended
16 information showing that usage of the decryption key has
17 ended.

1 12. The terminal apparatus of claim 11, further comprising:
2 a usage unit operable to decrypt the encrypted content
3 using the decryption key to generate a content, and to use
4 the content, wherein
5 the detecting unit detects the end of content usage by
6 the usage unit.

1 13. The terminal apparatus of claim 12, wherein
2 the key reception unit includes a decryption subunit
3 operable, when the decryption key is to be received, to
4 receive an encrypted decryption key, and to decrypt the
5 encrypted decryption key to generate the decryption key.

1 14. The terminal apparatus of claim 11, wherein
2 the key reception unit further receives a key-usage
3 period of the decryption key from the key delivery apparatus,
4 the terminal apparatus manages a content-usage period,
5 and further comprises a period judging unit operable to judge

6 whether the key-usage period has expired, and
7 the detecting unit detects that content usage has ended
8 when judged that the key-usage period has expired.

1 15. The terminal apparatus of claim 12, wherein
2 the key reception unit includes a decryption subunit
3 operable, when the decryption key and a key-usage period of
4 the decryption key are to be received, to receive an encrypted
5 decryption key and an encrypted key-usage period, and to
6 decrypt the encrypted decryption key and the encrypted
7 key-usage period to generate the decryption key and the
8 key-usage period.

1 16. The terminal apparatus of claim 11, further comprising:
2 a proprietary judging unit operable to receive, from
3 the key delivery apparatus, search information showing the
4 decryption key, and to judge whether the decryption key is
5 held in the terminal apparatus, using the search information;
6 and
7 a proprietary notifying unit operable, when judged that
8 the decryption key is held in the terminal apparatus, to
9 notify to the key delivery apparatus, information indicating
10 that the decryption key is held in the terminal apparatus.

1 17. A portable recording medium that receives supply of a
2 decryption key for decrypting an encrypted content from a
3 key delivery apparatus that manages the decryption key,
4 comprising:

5 a key reception unit operable to receive the decryption
6 key and a key-usage period of the decryption key from the
7 key delivery apparatus, when judged in the key delivery
8 apparatus that supply of the decryption key is possible; and

9 a key-information storage unit operable to store the
10 decryption key and the key-usage period.

1 18. The recording medium of claim 17, wherein

2 the key reception unit includes a decryption subunit
3 operable, when the decryption key and the key-usage period
4 of the decryption key are to be received, to receive an
5 encrypted decryption key and an encrypted key-usage period,
6 and to decrypt the encrypted decryption key and the encrypted
7 key-usage period to generate the decryption key and the
8 key-usage period.

1 19. The recording medium of claim 17, further comprising:

2 a period judging unit operable to judge whether the
3 key-usage period has expired; and

4 a deletion unit operable to delete the decryption key

5 and the key-usage period when judged that the key-usage
6 period has expired.

1 20. The recording medium of claim 17, further comprising:
2 a proprietary judging unit operable to receive, from
3 the key delivery apparatus, search information showing the
4 decryption key, and to judge whether the decryption key is
5 held in the recording medium, using the search information;
6 and
7 a proprietary notifying unit operable, when judged that
8 the decryption key is held in the recording medium, to notify
9 to the key delivery apparatus, information indicating that
10 the decryption key is held in the recording medium.

1 21. A key delivery system comprising (i) a key delivery
2 apparatus that manages a decryption key for decrypting an
3 encrypted content and a suppliable number showing how many
4 times the decryption key is suppliable, with respect to a
5 terminal apparatus connected to a network, (ii) a first-type
6 terminal apparatus that manages a content-usage period, and
7 (iii) a second-type terminal apparatus that does not manage
8 the content-usage period, the key management apparatus
9 including:

10 a receiving unit operable to receive, from the terminal

11 apparatus, a supply request for the decryption key;
12 a supply judging unit operable, if the terminal
13 apparatus is a legitimate supply target, to judge whether
14 the terminal apparatus is one of the first-type terminal
15 apparatus and the second-type terminal apparatus; and
16 a key supply unit operable, if the suppliable number
17 has a remaining number, to supply to the terminal apparatus,
18 the decryption key and a key-usage period of the decryption
19 key when judged that the terminal apparatus is the first-type
20 terminal apparatus and the decryption key when judged that
21 the terminal apparatus is the second-type terminal apparatus,
22 wherein
23 the supply judging unit judges the terminal apparatus
24 to be the first-type terminal apparatus if the terminal
25 apparatus records the encrypted content, the decryption key,
26 and the key-usage period onto a portable recording medium,
27 the first-type terminal apparatus receives from the key
28 delivery apparatus and stores the decryption key and the
29 key-usage period, and
30 the second-type terminal apparatus receives the
31 decryption key from the key delivery apparatus, and uses the
32 decryption key in content usage.

1 22. A key supply method used in a key delivery apparatus that

2 manages a decryption key for decrypting an encrypted content
3 and a suppliable number showing how many times the decryption
4 key is suppliable, with respect to a terminal apparatus
5 connected to a network, comprising the steps of:

6 receiving, from the terminal apparatus, a supply
7 request for the decryption key;

8 judging, if the terminal apparatus is a legitimate
9 supply target, whether the terminal apparatus is one of a
10 first-type terminal apparatus that manages a content-usage
11 period and a second-type terminal apparatus that does not
12 manage the content-usage period; and

13 supplying to the terminal apparatus, if the suppliable
14 number has a remaining number, the decryption key and a
15 key-usage period of the decryption key when judged that the
16 terminal apparatus is the first-type terminal apparatus and
17 the decryption key when judged that the terminal apparatus
18 is the second-type terminal apparatus.

1 23. A key supply computer program used in a key delivery
2 apparatus that manages a decryption key for decrypting an
3 encrypted content and a suppliable number showing how many
4 times the decryption key is suppliable, with respect to a
5 terminal apparatus connected to a network, comprising the
6 steps of:

7 receiving, from the terminal apparatus, a supply
8 request for the decryption key;
9 judging, if the terminal apparatus is a legitimate
10 supply target, whether the terminal apparatus is one of a
11 first-type terminal apparatus that manages a content-usage
12 period and a second-type terminal apparatus that does not
13 manage the content-usage period; and
14 supplying to the terminal apparatus, if the suppliable
15 number has a remaining number, the decryption key and a
16 key-usage period of the decryption key when judged that the
17 terminal apparatus is the first-type terminal apparatus and
18 the decryption key when judged that the terminal apparatus
19 is the second-type terminal apparatus.

1 24. A computer-readable recording medium storing a key supply
2 computer program used in a key delivery apparatus that
3 manages a decryption key for decrypting an encrypted content
4 and a suppliable number showing how many times the decryption
5 key is suppliable, with respect to a terminal apparatus
6 connected to a network, the computer program comprising the
7 steps of:

8 receiving, from the terminal apparatus, a supply
9 request for the decryption key;
10 judging, if the terminal apparatus is a legitimate

11 supply target, whether the terminal apparatus is one of a
12 first-type terminal apparatus that manages a content-usage
13 period and a second-type terminal apparatus that does not
14 manage the content-usage period; and
15 supplying to the terminal apparatus, if the suppliable
16 number has a remaining number, the decryption key and a
17 key-usage period of the decryption key when judged that the
18 terminal apparatus is the first-type terminal apparatus and
19 the decryption key when judged that the terminal apparatus
20 is the second-type terminal apparatus.